

IMPROVED SYSTEM AND METHOD FOR PROVIDING ANSWERS IN A PERSONAL ENTROPY SYSTEM

ABSTRACT OF THE DISCLOSURE

Computer user authentication and cryptographic key protection through
5 the use of personal entropy (PE) is implemented using a PE answering algorithm
which enables a user of a computing system to generate secret values from
answers to questions previously created by the user. The questions are displayed
to the user on a user interface (UI), and the user is prompted to select a subset of
the questions to answer. When the user provides answers for the selected subset,
10 an attempt is made to generate the secret value from a portion of the subset and
possibly other information. If the secret value cannot be generated from at least a
portion of the selected subset, the user is prompted to select a second subset of
the displayed questions and provide answers to the selected second set of
questions. When the user provides answers to the second selected subset of
15 questions, an attempt is made to generate the secret value from a portion of the
first and second sets of answers and possibly other information. The hardware
implementation of PE answering algorithm has three components; the PE-
controller server computer, the PE-user client controller and the PE-
authentication server computer. These components are interconnected via a
20 network. Attached to the PE-controller server is a repository of downloadable
client applets which are downloaded to the PE-user client controller and used for
both creating the secret value from answers supplied by the user when creating the
questions in the create PE process and, later, in the recover PE process,
generating the secret value from answers provided by the user to subsets of the
25 previously created questions. The PE-authentication server computer maintains a
central database where PE information created by PE users can be stored and
subsequently accessed by the PE-controller server computer. The
PE-authentication server computer also performs a user authentication service.